Spis treści

O autorach 11
O korektorze merytorycznym 11
Podziękowania 12

PRZEDMOWA **13**
WSTĘP **15**

1
PRZYGOTOWANIE ŚRODOWISKA PYTHONA **17**
Instalowanie systemu Kali Linux 17
Konfigurowanie języka Python 3 18
Instalowanie środowiska programistycznego 21
Higiena kodu 22

2
PODSTAWOWE NARZĘDZIA SIECIOWE **25**
Narzędzia sieciowe Pythona 26
Klient TCP 26
Klient UDP 27
Serwer TCP 28
Budowa netcata 29
Czy to w ogóle działa 33
Tworzenie proxy TCP 35
Czy to w ogóle działa 41
SSH przez Paramiko 42
Czy to w ogóle działa 47
Tunelowanie SSH 47
Czy to w ogóle działa 50

3
TWORZENIE SZPERACZA SIECIOWEGO **53**
Budowa narzędzia UDP do wykrywania hostów 54
Tropienie pakietów w Windowsie i Linuksie 54
Czy to w ogóle działa 56
Dekodowanie warstwy IP 56
Moduł ctypes 57
Moduł struct 58

Tworzenie dekodera IP 61
Czy to w ogóle działa 62
Dekodowanie danych ICMP 63
Czy to w ogóle działa 68

4
WŁADANIE SIECIĄ ZA POMOCĄ SCAPY 69
Wykradanie danych poświadczających użytkownika z wiadomości e-mail 70
Czy to w ogóle działa 73
Atak ARP cache poisoning przy użyciu biblioteki Scapy 73
Czy to w ogóle działa 78
Przetwarzanie pliku PCAP 80
Czy to w ogóle działa 86

5
HAKOWANIE APLIKACJI SIECIOWYCH 87
Biblioteki internetowe 88
Biblioteka urllib2 dla Pythona 2.x 88
Biblioteka urllib dla Pythona 3.x 89
Biblioteka requests 90
Pakiety lxml i BeautifulSoup 90
Mapowanie aplikacji sieciowych typu open source 92
Mapowanie platformy WordPress 93
Testowanie rzeczywistej witryny 96
Czy to w ogóle działa 97
Analizowanie aplikacji metodą siłową 98
Czy to w ogóle działa 101
Ataki siłowe na formularze uwierzytelniania 102
Czy to w ogóle działa 107

6
ROZSZERZANIE NARZĘDZI BURP 109
Wstępna konfiguracja 110
Fuzzing przy użyciu Burpa 111
Czy to w ogóle działa 116
Bing w służbie Burpa 121
Czy to w ogóle działa 124
Treść strony internetowej jako kopalnia haseł 125
Czy to w ogóle działa 129

7
CENTRUM DOWODZENIA GITHUB 133
Tworzenie konta w portalu GitHub 134
Tworzenie modułów 135
Konfiguracja trojana 136
Budowa trojana komunikującego się z portalem GitHub 137
Hakowanie funkcji importu Pythona 139
Czy to w ogóle działa 141

8
POPULARNE ZADANIA TROJANÓW W SYSTEMIE WINDOWS 143
Rejestrowanie naciskanych klawiszy 144
Czy to w ogóle działa 146
Robienie zrzutów ekranu 147
Wykonywanie kodu powłoki przy użyciu Pythona 148
Czy to w ogóle działa 150
Wykrywanie środowiska ograniczonego 151

9
ZABAWA W WYPROWADZANIE DANYCH 155
Szyfrowanie i deszyfrowanie plików 156
Wyprowadzanie danych za pomocą poczty e-mail 159
Wyprowadzanie danych za pomocą transferu plików 160
Wyprowadzanie danych do serwera WWW 161
Wszystko razem 165
Czy to w ogóle działa 166

10
ZWIĘKSZANIE UPRAWNIEŃ W SYSTEMIE WINDOWS 169
Instalacja potrzebnych narzędzi 170
Tworzenie testowej usługi BlackHat 170
Tworzenie monitora procesów 173
Monitorowanie procesów przy użyciu WMI 173
Czy to w ogóle działa 175
Uprawnienia tokenów Windows 176
Pierwsi na mecie 178
Czy to w ogóle działa 181
Wstrzykiwanie kodu 181
Czy to w ogóle działa 183

11
OFENSYWNA ANALIZA ŚLEDCZA 185
Instalacja 186
Ogólny rekonesans 187
Rekonesans użytkowników 189
Rekonesans słabych punktów 191
Interfejs volshell 193
Własne wtyczki dla Volatility 193
Czy to w ogóle działa 198
Idź dalej! 200